CLAIMS

What is claimed is:

1. A method comprising:

receiving a request to prove that a platform possesses cryptographic information from a certifying manufacturer; and

performing a direct proof by the platform to prove that the platform possesses the cryptographic information, the direct proof comprises a plurality of exponentiations each being conducted using an exponent having a bit length no more than one-half a bit length of a modulus (n).

2. The method of claim 1, wherein the bit length of the exponent being at most 160 bits in length.

3. The method of claim 1, wherein the modulus (n) being over 1000 bits in length.

4. The method of claim 1, wherein the bit length of the exponent being a constant value despite any increase in value of the modulus (n).

5. The method of claim 1, wherein the bit length of the exponent being less than one-eighth the bit length of the modulus (n).

6. The method of claim 1, wherein the plurality of exponentiations conducted are of the form h^t mod P, where "h" is a unique number, "t" is randomly chosen between an interval between 0 and W, "P" is a large prime number, and W is a number between 2^{80} and the square root of n.

7. A method comprising:

receiving a request to prove that a platform possesses cryptographic information from a certifying manufacturer; and

performing a direct proof by the platform to prove that the platform possesses the cryptographic information, the direct proof comprises a plurality of exponentiations each being conducted using an exponent remaining constant despite an increase in a bit length of a modulus (n).

8. The method of claim 7, wherein the bit length of the exponent being less than one-sixth of the bit length of the modulus (n).

9. The method of claim 7, wherein the bit length of the exponent being at most 160 bits in length.

10. The method of claim 9, wherein the modulus (n) being over 1000 bits in length.

11. The method of claim 7, wherein each of the plurality of exponentiations conducted are of the form h^t mod P, where "h" is a unique number, "t" is randomly chosen between an interval between 0 and W, "P" is a large prime number, and W is a number between 2^{80} and the square root of n.

12. The method of claim 11, wherein the value "t" is of a form y^e mod n, where "e" is a public exponent and "y" is either a random or pseudo-randomly chosen number within an interval ranging from 0 to n.

13. A method comprising:

receiving a request for information by a cryptographic device; and

proving in a single direct proof that a value was signed by a signature key without revealing the value, the single direct proof comprises a plurality of exponentiations of which all of the plurality of exponentiations are conducted using a fixed exponent substantially less in bit length than a bit length of a modulus (n).

14. The method of claim 13, wherein the bit length of the exponent being at most 160 bits in length.

15. The method of claim 14, wherein the modulus (n) is over 1000 bits in length.

16. The method of claim 13, wherein the bit length of the fixed exponents associated with the exponentiations are a constant value despite any increase in value of the modulus (n).

17. A platform comprising:

a bus;

a network interface card coupled to the bus; and

a processor coupled to the bus; and

a trusted platform module coupled to the processor, in response to a challenge received over the network interface card, the trusted platform module to perform a direct proof in order to prove that the trusted platform module has a digital signature from a device manufacturer and the digital signature is valid without revealing the digital signature, the direct proof comprises a plurality of exponentiations each being conducted using an exponent having a bit length no more than one-half a bit length of a modulus (n).

18. The platform of claim 17, wherein the direct proof performed by the trusted platform module is conducted with the bit length of each exponent associated with all of the plurality of exponentiations being at most 160 bits in length.

19. The platform of claim 17, wherein the direct proof performed by the trusted platform module is conducted with the bit length of each exponent associated with all of the plurality of exponentiations being a constant value despite any increase in value of the modulus (n).